BANCO DE ESPAÑA
Eurosistema

Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES)

(EBA/GL/2017/05)

Estas Directrices de la Autoridad Bancaria Europea (EBA por sus siglas en inglés) van dirigidas a las autoridades competentes definidas en el artículo 4, apartado 2, inciso i), del Reglamento (UE) nº 1093/2010.

Las Directrices tienen por objeto lograr la convergencia de las prácticas de supervisión en la evaluación del riesgo de las Tecnologías de la Información y la Comunicación (TIC) en el marco del Proceso de Revisión y Evaluación Supervisora (PRES) mencionado en el artículo 97 de la Directiva 2013/36/UE. En particular, especifican los criterios que las autoridades competentes deberían aplicar en la evaluación supervisora del gobierno y la estrategia en materia de TIC de las entidades y en la evaluación supervisora de las exposiciones al riesgo de TIC y los controles correspondientes de las entidades.

Las autoridades competentes deberían aplicar estas Directrices en consonancia con el nivel de aplicación del PRES especificado en las Directrices de la EBA sobre el PRES, y de conformidad con el principio de proporcionalidad establecido en las mismas.

Estas Directrices han sido desarrolladas por la EBA a iniciativa propia de acuerdo con lo señalado en el artículo 16 del Reglamento (UE) No 1093/2010. La EBA publicó la versión en inglés de mismas el 11 de mayo de 2017 y la versión en español el 11 de septiembre de 2017. Las Directrices se aplicarán a partir del 1 de enero de 2018.

La Comisión Ejecutiva del Banco de España, en su calidad de autoridad competente de la supervisión directa de las entidades menos significativas, adoptó estas Directrices como propias el día 7 de noviembre de 2017.

EBA/GL/2017/05

11/09/2017

Directrices

Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES)

1. Obligaciones de cumplimiento y de notificación

Rango jurídico de las presentes directrices

1. El presente documento contiene directrices emitidas en virtud del artículo 16 del Reglamento (UE) nº 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) nº 1093/2010, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a ellas.

2. En las directrices se expone el punto de vista de la ABE sobre las prácticas de supervisión más adecuadas en el marco del Sistema Europeo de Supervisión Financiera o sobre cómo debería aplicarse el Derecho de la Unión en un determinado ámbito. Las autoridades competentes definidas en el artículo 4, apartado 2, del Reglamento (UE) nº 1093/2010 a las que sean de aplicación las directrices deberían cumplirlas incorporándolas a sus prácticas de la forma más apropiada (modificando, por ejemplo, su marco jurídico o sus procedimientos de supervisión), incluso en aquellos casos en los que las directrices vayan dirigidas principalmente a las entidades.

Requisitos de notificación

3. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) nº 1093/2010, las autoridades competentes deberán notificar a la ABE, a más tardar el 13.11.2017, si cumplen o se proponen cumplir estas directrices indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en dicho plazo, la ABE considerará que las autoridades competentes no las cumplen. Las notificaciones se presentarán remitiendo el modelo que se encuentra disponible en el sitio web de la ABE a compliance@eba.europa.eu, con la referencia «EBA/GL/2017/05». Las notificaciones serán presentadas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes. Cualquier cambio en la situación de cumplimiento de las directrices deberá notificarse igualmente a la ABE.

4. Las notificaciones se publicarán en el sitio web de la ABE, tal y como contempla el artículo 16, apartado 3.

[1] Reglamento (UE) nº 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión nº 2009/78/CE de la Comisión, (DO L 331 de 15.12.2010, p. 12).

2. Objeto, ámbito de aplicación y definiciones

Objeto y ámbito de aplicación

5. Las presentes Directrices, elaboradas de conformidad con el artículo 107, apartado 3, de la Directiva 2013/36/UE[2], tienen por objeto lograr la convergencia de las prácticas de supervisión en la evaluación del riesgo de las tecnologías de la información y la comunicación (TIC) en el marco del proceso de revisión y evaluación supervisora (PRES) mencionado en el artículo 97 de la Directiva 2013/36/UE, y que se detalla de manera más pormenorizada en las Directrices de la ABE sobre procedimientos y metodologías comunes para el proceso de revisión y evaluación supervisora (PRES)[3]. En particular, las presentes Directrices especifican los criterios de evaluación que las autoridades competentes deberían aplicar en la evaluación supervisora del gobierno y la estrategia en materia de TIC de las entidades y en la evaluación supervisora de las exposiciones al riesgo de TIC y los controles correspondientes de las entidades. Las presentes Directrices forman parte integrante de las Directrices de la ABE sobre el PRES.

6. Las autoridades competentes deberían aplicar estas Directrices en consonancia con el nivel de aplicación del PRES especificado en las Directrices de la ABE sobre el PRES y de conformidad con los requisitos de proporcionalidad y el enfoque de la dedicación mínima establecidos en las mismas.

Destinatarios

7. Las presentes Directrices se dirigen a las autoridades competentes definidas en el artículo 4, apartado 2, letra i), del Reglamento (UE) n.º 1093/2010.

Definiciones

8. Salvo que se indique lo contrario, los términos utilizados y definidos en la Directiva 2013/36/UE y en el Reglamento (UE) n.º 575/2013 y las definiciones de las Directrices de la ABE sobre el PRES tendrán el mismo significado en las presentes Directrices. Además, a los efectos de estas Directrices, se entenderá por:

[2] Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (1) - DO L 176 de 27.6.2013.

[3] EBA/GL/2014/13

Sistemas de TIC	Configuración de los elementos de las TIC como parte de un mecanismo o una red de interconexión que sirve de soporte para las operaciones de una entidad.
Servicios de TIC	Servicios prestados por sistemas de TIC a uno o más usuarios internos o externos. Algunos ejemplos serían los servicios de entrada, almacenamiento y tratamiento de datos y los servicios de información, pero también los servicios de monitorización y de soporte al negocio y a la toma de decisiones.
Riesgo de disponibilidad y continuidad de las TIC	El riesgo de que el rendimiento y la disponibilidad de los sistemas de TIC y los datos se vean afectados negativamente, incluida la incapacidad para recuperar oportunamente los servicios de la entidad, debido a un fallo de los componentes de *hardware* o *software* de las TIC; debilidades en la gestión de los sistemas de TIC; o cualquier otra circunstancia, tal como se detalla en el anexo.
Riesgo de seguridad de las TIC	El riesgo de acceso no autorizado a los sistemas de TIC y a los datos dentro y fuera de la entidad (por ejemplo, ciberataques), como se detalla en el anexo.
Riesgo de cambio de las TIC	El riesgo derivado de la incapacidad de la entidad para gestionar de forma oportuna y controlada los cambios en los sistemas de TIC, sobre todo en el caso de programas de cambio grandes y complejos, como se detalla en el anexo.
Riesgo de integridad de datos TIC	El riesgo de que los datos almacenados y procesados por los sistemas de TIC sean incompletos, inexactos o incoherentes en los diferentes sistemas de TIC —por ejemplo, como resultado de la deficiencia o inexistencia de controles de TIC durante las diferentes fases del ciclo de vida de los datos (es decir, diseño de la arquitectura de datos, construcción del modelo de datos o de los diccionarios de datos, verificación de los datos de entrada, control de las extracciones, transferencias y procesamientos de datos, incluidos los datos de salida obtenidos)—, reduciendo la capacidad de una entidad para prestar servicios y producir información de gestión (de riesgos) y financiera de manera correcta y oportuna, como se detalla en el anexo.
Riesgo de externalización de las TIC	El riesgo de que la contratación de sistemas de TIC o servicios relacionados a un tercero u otra entidad del grupo (subcontratación intragrupo) tenga un efecto negativo en el desempeño de la entidad y la gestión de riesgos, como se detalla en el anexo.

3. Aplicación

Fecha de aplicación

9. Estas Directrices serán de aplicación a partir del 1 de enero de 2018.

4. Requisitos para la evaluación del riesgo de TIC

Título 1 - Disposiciones generales

10. Las autoridades competentes realizarán la evaluación del riesgo de TIC y de los procedimientos de gobierno y la estrategia de TIC como parte del PRES, siguiendo el enfoque de dedicación mínima y los criterios de proporcionalidad especificados en el título 2 de las Directrices de la ABE sobre el PRES. En particular, esto significa que:

    a. la frecuencia de la evaluación del riesgo de TIC dependerá, siguiendo el enfoque de dedicación mínima, de la clase a la que esté asignada una entidad a efectos del PRES y de su programa de examen supervisor específico; y

    b. la profundidad, el detalle y la intensidad de la evaluación de las TIC serán proporcionales al tamaño, la estructura y el entorno operativo de la entidad, así como a la naturaleza, la escala y la complejidad de sus actividades.

11. En las presentes Directrices se aplica el principio de proporcionalidad al alcance, la frecuencia y la intensidad de la dedicación supervisora y del diálogo con la entidad y a las expectativas supervisoras de los criterios que debe cumplir dicha entidad.

12. Las autoridades competentes podrán utilizar y tomar en consideración los trabajos ya realizados por la entidad o por la autoridad competente en el contexto de las evaluaciones de otros riesgos o elementos del PRES a fin de tener una visión actualizada de la evaluación. En concreto, al realizar las evaluaciones especificadas en estas Directrices, las autoridades competentes seleccionarán el enfoque de evaluación supervisora más adecuado y la metodología que mejor se ajuste a la entidad aplicando el criterio de proporcionalidad. Las autoridades competentes utilizarán la documentación existente y disponible (por ejemplo, informes pertinentes y otros documentos, reuniones con los responsables de gestión (del riesgo), resultados de la inspección *in situ*) como base para su evaluación.

13. Las autoridades competentes resumirán los resultados de sus evaluaciones de los criterios especificados en estas Directrices y los utilizarán con el fin de extraer conclusiones sobre la evaluación de los elementos del PRES especificados en las Directrices de la ABE sobre el PRES.

14. En particular, la evaluación del gobierno y de la estrategia de TIC realizada de conformidad con el título 2 de las presentes Directrices generará resultados que se tendrán en cuenta en el resumen de los resultados de la evaluación del gobierno interno y de los controles globales en el marco del PRES, tal como se especifica en el título 5 de las Directrices de la ABE sobre el PRES, y se reflejarán en la puntuación de ese elemento del PRES. Asimismo, las autoridades competentes tendrán en cuenta que

cualquier impacto adverso significativo que la evaluación de la estrategia de TIC pueda tener sobre la estrategia de negocio de la entidad, o cualquier preocupación respecto a que la entidad no tenga suficientes recursos y capacidades de TIC para llevar a cabo y dar soporte a cambios estratégicos importantes previstos deberán incorporarse al análisis del modelo de negocio de conformidad con el título 4 de las Directrices de la ABE sobre el PRES.

15. El resultado de la evaluación del riesgo de TIC, tal como se especifica en el título 3 de estas Directrices, servirá de base para obtener los resultados de la evaluación del riesgo operacional y para determinar la puntuación pertinente, como se especifica en el título 6.4 de las Directrices de la ABE sobre el PRES.

16. Cabe señalar que, si bien las autoridades competentes evaluarán las subcategorías de riesgos como parte de las categorías principales (es decir, el riesgo de TIC se evaluará como parte del riesgo operacional), cuando consideren que algunas subcategorías son materiales, pueden evaluarlas de manera individual. Con este fin, si las autoridades competentes identifican el riesgo de TIC como riesgo material, las presentes Directrices también proporcionan un cuadro de puntuaciones (cuadro 1) que se utilizará para asignar una puntuación independiente a la subcategoría de riesgo de TIC, de conformidad con el enfoque general sobre la puntuación de los riesgos para el capital que figura en las Directrices de la ABE sobre el PRES.

17. A fin de determinar si el riesgo de TIC debe considerarse material y, por lo tanto, debería evaluarse y puntuarse como subcategoría individual del riesgo operacional, las autoridades competentes pueden usar los criterios especificados en la sección 6.1 de las Directrices de la ABE sobre el PRES.

18. Al aplicar estas Directrices, las autoridades competentes deberán considerar, cuando proceda, la lista no exhaustiva de subcategorías y escenarios de riesgo de TIC que figuran en el anexo, observando que el anexo se centra en los riesgos de TIC que pueden dar lugar a pérdidas muy graves. Las autoridades competentes pueden excluir algunos de los riesgos de TIC incluidos en la taxonomía si no son pertinentes para su evaluación. Se espera que las entidades mantengan sus propias taxonomías de riesgo en lugar de utilizar la taxonomía de riesgos de TIC presentada en el anexo.

19. Cuando estas Directrices se apliquen en relación con grupos bancarios transfronterizos y sus entidades y se haya creado un colegio de supervisores, las autoridades competentes implicadas, en el contexto de su cooperación para la evaluación del PRES de conformidad con la sección 11.1 de las Directrices de la ABE sobre el PRES, coordinarán, en la medida de lo posible, el alcance exacto y detallado de cada elemento de información de manera coherente para todas las entidades del grupo.

Título 2 - Evaluación del gobierno y de la estrategia de TIC de la entidad

2.1 Principios generales

20. Las autoridades competentes evaluarán si el marco general de gobierno y control interno de la entidad cubre debidamente los sistemas de TIC y los riesgos relacionados y si el órgano de dirección trata y gestiona adecuadamente estos aspectos, ya que las TIC son parte integrante del buen funcionamiento de una entidad.

21. Al realizar esta evaluación, las autoridades competentes consultarán los requisitos y normas de buen gobierno interno y los procedimientos de control de riesgos, como se especifica en la Guía de la ABE sobre gobierno interno (GL 44)[4], así como las orientaciones internacionales sobre la materia, en la medida en la que sean aplicables, dada la especificidad de los sistemas y riesgos de TIC.

22. La evaluación contemplada en este título no cubre los elementos específicos del gobierno, la gestión y los controles de riesgos de TIC que se centran en la gestión de los riesgos específicos de TIC abordados en el título 3 de estas Directrices, sino que se centra en las siguientes áreas:

    a. Estrategia de TIC: si la entidad cuenta con una estrategia de TIC adecuadamente gobernada y en línea con su estrategia de negocio;

    b. Gobierno interno general: si los procedimientos de gobierno interno generales de la entidad son adecuados en relación con sus sistemas de TIC; y

    c. El riesgo de TIC en el marco de gestión de riesgos de la entidad: si el marco de gestión de riesgos y control interno de la entidad protege adecuadamente los sistemas de TIC de la entidad.

23. La letra a) a la que se hace referencia en el apartado 22, en tanto en cuanto proporciona información sobre los elementos de gobierno de la entidad, deberá alimentar, fundamentalmente, la evaluación del modelo de negocio que se aborda en el título 4 de las Directrices de la ABE sobre el PRES. Las letras b) y c) complementan las evaluaciones de los temas cubiertos por el título 5 de las Directrices de la ABE sobre el PRES, por lo que la evaluación descrita en estas Directrices se incorporará a la evaluación correspondiente contemplada en el título 5 de las Directrices de la ABE sobre el PRES.

24. El resultado de esta evaluación se utilizará, cuando proceda, en la evaluación de la gestión y los controles de riesgos del título 3 de las presentes Directrices.

[4] Guía de la ABE sobre gobierno interno, GL 44, 27 de septiembre de 2011.

2.2 Estrategia de TIC

25. En esta sección, las autoridades competentes evaluarán si la entidad cuenta con una estrategia de TIC que: está sujeta a una supervisión adecuada por parte del órgano de dirección de la entidad; es coherente con la estrategia de negocio, en particular para mantener actualizadas sus TIC y planificar o aplicar cambios importantes y complejos en materia de TIC; y sirve de soporte para el modelo de negocio de la entidad.

2.2.1 Desarrollo e idoneidad de la estrategia de TIC

26. Las autoridades competentes evaluarán si la entidad dispone de un marco adecuado, proporcional a la naturaleza, escala y complejidad de sus actividades de TIC, para la preparación y el desarrollo de su estrategia de TIC. Al llevar a cabo esta evaluación, las autoridades competentes considerarán si:

    a. la alta dirección[5] de la línea o líneas de negocio se implica de manera adecuada en la definición de las prioridades estratégicas de TIC de la entidad y, a su vez, la alta dirección de la función de TIC tiene conocimiento del desarrollo, el diseño y la puesta en marcha de estrategias e iniciativas importantes para el negocio, con el fin de asegurar que los sistemas de TIC, los servicios de TIC y la función de TIC (es decir, los responsables de la gestión y el despliegue de estos sistemas y servicios) se mantengan permanentemente alineados con la estrategia de negocio de la entidad, y si las TIC están efectivamente actualizadas;

    b. la estrategia de TIC está documentada y respaldada por planes de ejecución concretos, en particular en lo que respecta a los hitos importantes y la planificación de los recursos (incluidos los recursos financieros y humanos), para garantizar que son realistas y permiten implementar dicha estrategia;

    c. la entidad actualiza periódicamente su estrategia de TIC, en particular si hay cambios en la estrategia de negocio, para asegurar que las TIC y los objetivos, planes y actividades del negocio a medio y largo plazo se mantienen alineados; y

    d. el órgano de dirección de la entidad aprueba la estrategia de TIC, los planes de ejecución y supervisa su aplicación.

2.2.2 Implementación de la estrategia de TIC

27. Si la estrategia de TIC de la entidad requiere que se apliquen cambios importantes y complejos en las TIC, o cambios con implicaciones significativas para el modelo de negocio de la entidad, las autoridades competentes evaluarán si la entidad cuenta con un marco de control adecuado a su tamaño, a sus actividades de TIC, así como al nivel de las actividades de cambio, que respalde la implementación efectiva de su estrategia de TIC. Al llevar a cabo esta evaluación, las autoridades competentes considerarán si el marco de control:

[5] Órgano de dirección y alta dirección según se definen en el artículo 3, apartados 7 y 9 respectivamente, de la Directiva 2013/36/UE de 26 de junio de 2013.

a. incluye los procesos de gobierno (por ejemplo, seguimiento y presentación de informes de avance y presupuesto) y los órganos pertinentes (por ejemplo, una oficina de gestión de proyectos [OGP], un grupo de dirección de TIC o equivalentes) para prestar un respaldo efectivo a la ejecución de los programas estratégicos de TIC;

b. ha definido y asignado las funciones y responsabilidades para la ejecución de los programas estratégicos de TIC, prestando especial atención a la experiencia de las principales partes interesadas en la organización, la dirección y el seguimiento de cambios importantes y complejos de TIC, así como la gestión de sus repercusiones generales sobre la organización y los recursos humanos (por ejemplo, gestión de la resistencia al cambio, formación, comunicación);

c. implica a las funciones independientes de control y auditoría interna para asegurar que los riesgos asociados con la ejecución de la estrategia de TIC se han identificado, evaluado y mitigado de manera efectiva y que el marco de gobierno en vigor para aplicar la estrategia de TIC es eficaz; y

d. contiene un proceso de planificación y de revisión de la planificación que proporciona flexibilidad para responder a cuestiones importantes identificadas (por ejemplo, problemas de ejecución o retrasos) o a circunstancias externas (por ejemplo, cambios importantes en el entorno de negocio, cuestiones tecnológicas o innovaciones) con el fin de asegurar una adaptación oportuna del plan de ejecución de la estrategia.

2.3 Gobierno interno general

28. De conformidad con el título 5 de las Directrices de la ABE sobre el PRES, las autoridades competentes evaluarán si la entidad cuenta con una estructura corporativa adecuada y transparente que sea idónea y si ha implantado procedimientos de gobierno interno adecuados. En lo que respecta en concreto a los sistemas de TIC y en consonancia con las Directrices de la ABE sobre gobierno interno, esta evaluación incluirá también un examen de si la entidad demuestra:

    a. que tiene una estructura organizativa sólida y transparente con responsabilidades claras en materia de TIC, incluido el órgano de dirección y sus comités, y que los principales responsables de TIC (por ejemplo, director de sistemas de información [CIO], director de operaciones [COO] o funciones equivalentes) tienen acceso adecuado, directo o indirecto, al órgano de dirección, a fin de garantizar que la información o las cuestiones importantes relacionadas con las TIC se comuniquen, se traten y se decidan de manera adecuada a nivel de dicho órgano; y

    b. que el órgano de dirección conoce y aborda los riesgos asociados con las TIC;

29. En relación con la sección 5.2 de las Directrices de la ABE sobre el PRES, las autoridades competentes evaluarán si la política y estrategia de externalización de las TIC de la entidad considera, cuando sea procedente, el impacto de dicha externalización sobre el modelo de negocio y el negocio de la entidad.

2.4 Riesgo de TIC en el marco de gestión de riesgos de la entidad

30. A la hora de evaluar la gestión de riesgos y los controles internos globales de la entidad, tal como se establece en el título 5 de las Directrices de la ABE sobre el PRES, las autoridades competentes considerarán si el marco de gestión de riesgos y de control interno de la entidad contempla adecuadamente sus sistemas de TIC de una manera proporcional al tamaño y las actividades de la entidad y a su perfil de riesgo de TIC tal como se define en el título 3. En particular, las autoridades competentes determinarán si:

    a. El apetito de riesgo y el ICAAP cubren los riesgos de TIC, como parte de la categoría más amplia de riesgo operacional, para definir la estrategia general de riesgo y determinar el capital interno; y

    b. los riesgos de TIC están dentro del ámbito de los marcos globales de gestión de riesgos y de control interno de la entidad.

31. Las autoridades competentes llevarán a cabo la evaluación mencionada en la letra a) anterior teniendo en cuenta tanto escenarios esperados como adversos, por ejemplo, los escenarios incluidos en las pruebas de resistencia supervisoras o en las llevadas a cabo específicamente para la entidad.

32. En lo que respecta en concreto a la letra b), las autoridades competentes evaluarán si las funciones independientes de control y de auditoría interna, descritas en los apartados 104 (a), 104 (d), 105 (a) y 105 (c) de las Directrices de la ABE sobre el PRES, son adecuadas para garantizar un nivel suficiente de independencia entre las funciones de TIC y las de control y auditoría, habida cuenta del tamaño y el perfil de riesgo de TIC de la entidad.

2.5 Resumen de resultados

33. Estos resultados se reflejarán en el resumen de resultados contemplado en el título 5 de las Directrices de la ABE sobre el PRES y formarán parte de la puntuación correspondiente, de acuerdo con las consideraciones del cuadro 3 de las Directrices de la ABE sobre el PRES.

34. En relación con la evaluación de la estrategia de TIC, se deben considerar los siguientes puntos al concluir la evaluación anterior:

    a. Si las autoridades competentes llegan a la conclusión de que el marco de gobierno de la entidad es insuficiente para desarrollar e implementar la estrategia de TIC de la entidad tal y como se describe en el punto 2.2, deberán tenerlo en cuenta en la evaluación del gobierno interno de la entidad contemplada en el título 5, apartado 87 a), de las Directrices de la ABE sobre el PRES;

    b. Si, a partir de las evaluaciones llevadas a cabo conforme al punto 2.2, las autoridades competentes llegan a la conclusión de que hay una discrepancia significativa entre la estrategia de TIC y la estrategia de negocio que podría tener un importante impacto negativo sobre los objetivos de negocio o financieros a largo plazo de la entidad, la sostenibilidad de esta o su modelo de negocio, o las áreas/líneas de negocio que se han identificado como más

importantes de conformidad con el apartado 62, letra a) de las Directrices de la ABE sobre el PRES, deberán tenerlo en cuenta al realizar la evaluación del modelo de negocio contemplada en el título 4 de las Directrices sobre el PRES en su apartado 70, letras b) y c); y

c. Si, a partir de las evaluaciones realizadas conforme al apartado 2.2, las autoridades competentes llegan a la conclusión de que es posible que la entidad no cuente con recursos y capacidad de implantación de TIC suficientes para ejecutar y dar soporte a los cambios estratégicos importantes previstos, deberán tenerlo en cuenta al realizar la evaluación del modelo de negocio contemplada en el título 4 de las Directrices de la ABE sobre el PRES en su apartado 70, letra b).

Título 3 - Evaluación de las exposiciones y controles de los riesgos de TIC de las entidades

3.1 Consideraciones generales

35. Las autoridades competentes evaluarán si la entidad ha identificado, evaluado y mitigado adecuadamente sus riesgos de TIC. Este proceso deberá formar parte del marco de gestión del riesgo operacional y será congruente con el enfoque aplicable a este riesgo.

36. Las autoridades competentes identificarán en primer lugar los riesgos de TIC inherentes materiales a los que la entidad está o podría estar expuesta y, a continuación, realizarán una evaluación de la eficacia del marco de gestión de los riesgos de TIC y de los procedimientos y controles de la entidad para mitigar estos riesgos. El resultado de la evaluación se reflejará en un resumen de resultados que sirve de base para determinar la puntuación del riesgo operacional de las Directrices del PRES. Cuando se considere que el riesgo de TIC es material y las autoridades competentes deseen asignar una puntuación individual, se utilizará el cuadro 1 para asignarle una puntuación como subriesgo del riesgo operacional.

37. A la hora de realizar la evaluación contemplada en este título, las autoridades competentes deberán utilizar todas las fuentes de información disponibles, como se establece en el apartado 127 del título 6 de las Directrices de la ABE sobre el PRES, por ejemplo, las actividades, informes y resultados de la gestión de riesgos de la entidad, como base para identificar sus prioridades de evaluación supervisora. Las autoridades competentes también utilizarán otras fuentes de información para llevar a cabo esta evaluación, incluidas, cuando sea pertinente, las siguientes:

    a. Autoevaluaciones del riesgo y de controles de TIC (si se proporciona en la información del ICAAP);
    b. Información de gestión relacionada con el riesgo de TIC presentada al órgano de dirección de la entidad por la función de gestión de riesgos, como, por ejemplo, informes periódicos sobre el riesgo de TIC e información específica de incidentes (incluida la contenida en la base de datos de pérdidas operacionales) o datos de exposición al riesgo de TIC;
    c. resultados de auditorías internas y externas relacionadas con las TIC comunicados al comité de auditoría de la entidad.

3.2 Identificación de riesgos de TIC materiales

38. Las autoridades competentes identificarán los riesgos de TIC materiales a los que la entidad está o podría estar expuesta y, para ello, seguirán las etapas que se indican a continuación.

3.2.1 Revisión del perfil de riesgo de TIC de la entidad

39. Al examinar el perfil de riesgo de TIC de la entidad, las autoridades competentes considerarán toda la información pertinente sobre sus exposiciones al riesgo de TIC, incluida la información a la que se refiere el apartado 37, y las deficiencias o debilidades significativas identificadas en la organización de las TIC y en los controles globales de la entidad llevados a cabo de conformidad con el título 2 de las presentes Directrices y, en su caso, revisarán esta información de manera proporcionada. Como parte de esta revisión, las autoridades competentes considerarán:

    a. El impacto potencial de una interrupción significativa en los sistemas de TIC de la entidad sobre el sistema financiero, ya sea a nivel nacional o internacional;
    b. si la entidad puede estar sujeta a riesgos de seguridad de TIC o a riesgos de disponibilidad y continuidad de las TIC debido a dependencias de internet, a la adopción de múltiples soluciones de TIC innovadoras u otros canales de distribución de negocio que pueden aumentar su vulnerabilidad frente a los ciberataques;
    c. si la entidad puede estar más expuesta a riesgos de seguridad de TIC, riesgos de disponibilidad y continuidad de las TIC, riesgos de integridad de datos TIC o riesgos de cambio de las TIC debido a la complejidad (por ejemplo, como resultado de fusiones o adquisiciones) o a la naturaleza obsoleta de sus sistemas de TIC;
    d. si la entidad está llevando a cabo cambios importantes en sus sistemas o en su función de TIC (por ejemplo, como resultado de fusiones, adquisiciones, desinversiones o la sustitución de sus sistemas básicos de TIC) que pueden afectar negativamente a la estabilidad o al funcionamiento ordenado de los sistemas de TIC y pueden dar lugar a riesgos materiales de disponibilidad y continuidad de las TIC, riesgos de seguridad de las TIC, riesgos de cambio de las TIC o riesgos de integridad de datos TIC;
    e. si la entidad ha subcontratado servicios de TIC o sistemas de TIC dentro o fuera del grupo que pueden exponerla a riesgos de externalización de las TIC materiales;
    f. si la entidad está aplicando medidas agresivas de reducción de costes de TIC que pueden dar lugar a una reducción de las inversiones y recursos de TIC y del conocimiento sobre TIC necesarios y pueden aumentar la exposición a todos los tipos de riesgos de TIC de la taxonomía;
    g. Si la localización de centros de operaciones/de datos de TIC importantes (por ejemplo, regiones, países) puede exponer a la entidad a desastres naturales (por ejemplo, inundaciones, terremotos), inestabilidad política o conflictos laborales y disturbios civiles que pueden dar lugar a un aumento sustancial de los riesgos de disponibilidad y continuidad de las TIC y de los riesgos de seguridad de las TIC.

3.2.2 Revisión de los sistemas y servicios de TIC críticos

40. Como parte del proceso para identificar los riesgos de TIC que podrían tener un impacto prudencial significativo en la entidad, las autoridades competentes deberán revisar la documentación de la entidad y formarse una opinión sobre qué sistemas y servicios de TIC son críticos para el adecuado funcionamiento, disponibilidad, continuidad y seguridad de las actividades esenciales de la entidad.

41. Para ello, las autoridades competentes revisarán la metodología y los procesos aplicados por la entidad para identificar los sistemas y servicios de TIC que son críticos, teniendo en cuenta que algunos sistemas y servicios de TIC pueden ser considerados críticos por la entidad desde una perspectiva de continuidad y disponibilidad de la actividad, o desde una perspectiva de seguridad (por ejemplo, prevención del fraude) o de confidencialidad (por ejemplo, datos confidenciales). Al realizar la revisión, las autoridades competentes tendrán en cuenta que los sistemas y servicios críticos de TIC deben cumplir al menos una de las siguientes condiciones:

    a. dan soporte a las principales operaciones de negocio y canales de distribución (por ejemplo, cajeros automáticos, banca por internet y banca móvil) de la entidad;

    b. prestan apoyo a los procesos de gobierno y las funciones corporativas esenciales, incluida la gestión de riesgos (por ejemplo, los sistemas de gestión de riesgos y sistemas de gestión de tesorería);

    c. están sujetos a requisitos jurídicos o regulatorios especiales (en su caso) que imponen mayores exigencias de disponibilidad, resiliencia, confidencialidad o seguridad (por ejemplo, legislación sobre protección de datos o posibles «objetivos de tiempo de recuperación» [RTO, el tiempo máximo dentro del cual un sistema o proceso debe ser restaurado después de un incidente] y «Objetivo de punto de recuperación» [RPO, el periodo máximo de datos que puede perderse en caso de que se produzca un incidente]) para algunos servicios importantes desde un punto de vista sistémico (en su caso);

    d. procesan o almacenan datos confidenciales o sensibles, cuyo acceso no autorizado podría afectar significativamente a la reputación de la entidad, los resultados financieros o la solidez y la continuidad de su negocio (por ejemplo, bases de datos con datos sensibles de los clientes); o

    e. proporcionan funcionalidades básicas que son vitales para el adecuado funcionamiento de la entidad (por ejemplo, servicios de telecomunicaciones y de conectividad, servicios de TIC y de ciberseguridad).

3.2.3 Identificación de riesgos de TIC materiales para los sistemas y servicios de TIC críticos

42. Teniendo en cuenta las revisiones del perfil de riesgo de TIC y de los sistemas y servicios de TIC críticos de la entidad arriba mencionadas, las autoridades competentes deberán formarse una opinión sobre los riesgos de TIC materiales que, a su juicio, pueden tener un impacto prudencial significativo en los sistemas y servicios de TIC críticos de la entidad.

43. Al evaluar el impacto potencial de los riesgos de TIC en los sistemas y servicios de TIC críticos de la entidad, las autoridades competentes tendrán en cuenta:

    a. El impacto financiero, incluyendo (entre otros) la pérdida de fondos o activos, las posibles compensaciones a clientes, los costes legales y de reparación, los daños y perjuicios contractuales, la pérdida de ingresos;

b. La probabilidad de interrupción del negocio, considerando (entre otros aspectos) la criticidad de los servicios financieros afectados; el número de clientes o sucursales y de empleados potencialmente afectados;

c. El impacto potencial sobre la reputación de la entidad en función de la criticidad del servicio bancario o de la actividad operativa afectada (por ejemplo, el robo de datos de clientes); el perfil/visibilidad externa de los sistemas y servicios de TIC afectados (por ejemplo, sistemas bancarios móviles o por internet, puntos de venta, cajeros automáticos o sistemas de pago);

d. El impacto regulatorio, incluida la probabilidad de censura pública por parte del regulador, multas o incluso la modificación de los permisos.

e. El impacto estratégico en la entidad, por ejemplo, si se comprometen o roban los planes estratégicos de producto o de negocio.

44. Posteriormente, las autoridades competentes asignarán los riesgos de TIC identificados que se consideran materiales a las siguientes categorías de riesgo de TIC, para las cuales se proporcionan descripciones y ejemplos adicionales en el anexo. Las autoridades competentes deberán considerar los riesgos de TIC descritos en el anexo como parte de la evaluación del título 3:

a. Riesgo de disponibilidad y de continuidad de las TIC
b. Riesgo de seguridad de las TIC
c. Riesgo de cambio de las TIC
d. Riesgo de integridad de datos TIC
e. Riesgo de externalización de las TIC

La asignación tiene como fin ayudar a las autoridades competentes a determinar qué riesgos son materiales (en su caso) y, por lo tanto, deben someterse a una revisión más profunda o pormenorizada en las etapas siguientes de evaluación.

3.3 Evaluación de los controles para mitigar los riesgos de TIC materiales

45. A fin de evaluar la exposición residual de la entidad al riesgo de TIC, las autoridades competentes revisarán la forma en que la entidad identifica, sigue, evalúa y mitiga los riesgos materiales que han identificado en la evaluación anterior.

46. Con este fin, para los riesgos de TIC materiales identificados, las autoridades competentes revisarán lo siguiente:

a. Política de gestión del riesgo de TIC, procesos y umbrales de tolerancia al riesgo;

b. Marco de gestión y supervisión de la organización;

c. Cobertura de auditoría interna y conclusiones; y

d. Controles específicos para los riesgos de TIC materiales identificados.

47. La evaluación tendrá en cuenta los resultados del análisis del marco general de gestión de riesgos y de control interno al que se refiere el título 5 de las Directrices de la ABE sobre el PRES, así como el gobierno y la estrategia de la entidad contemplados en el título 2 de las presentes Directrices, dado que las deficiencias significativas identificadas en estas áreas pueden influir en la capacidad de la entidad para gestionar y mitigar sus exposiciones al riesgo de TIC. Cuando proceda, las autoridades competentes también deberán utilizar las fuentes de información que figuran en el apartado 37 de las presentes Directrices.

48. Las autoridades competentes llevarán a cabo las siguientes etapas de evaluación de manera proporcional a la naturaleza, la escala y la complejidad de las actividades de la entidad, efectuando una revisión supervisora adecuada al perfil de riesgo de TIC de la entidad.

3.3.1 Política de gestión del riesgo de TIC, procesos y umbrales de tolerancia al riesgo

49. Las autoridades competentes revisarán si la entidad cuenta con políticas, procesos y umbrales de tolerancia adecuados para la gestión de los riesgos de TIC materiales identificados. Pueden formar parte del marco de gestión del riesgo operacional o estar recogidos en un documento separado. Al llevar a cabo esta evaluación, las autoridades competentes considerarán si:

    a. El órgano de dirección formaliza y aprueba la política de gestión de riesgos y esta contiene suficientes orientaciones sobre el apetito de riesgo de TIC de la entidad y sobre los principales objetivos perseguidos en materia de gestión de riesgos de TIC o los límites de tolerancia al riesgo de TIC aplicados. Además, la política de gestión del riesgo de TIC pertinente deberá ser comunicada a todas las partes interesadas relevantes;

    b. la política aplicable abarca todos los elementos significativos para la gestión de los riesgos de TIC materiales identificados;

    c. la entidad ha puesto en marcha un proceso y los correspondientes procedimientos para la identificación (por ejemplo, «autoevaluaciones de control de riesgos» [RCSA] y análisis de escenarios de riesgo) y monitorización de los riesgos de TIC materiales; y

    d. la entidad cuenta con un sistema de información de gestión de riesgos de TIC que proporciona información oportuna a la alta dirección y al órgano de dirección y que les permite evaluar y monitorizar si los planes y las medidas de mitigación del riesgo de TIC de la entidad son coherentes con los umbrales de apetito o tolerancia al riesgo aprobados (cuando sea pertinente), así como monitorizar los cambios en los riesgos de TIC materiales.

3.3.2 Marco de gestión y supervisión de la organización

50. Las autoridades competentes evaluarán cómo las funciones y responsabilidades de gestión de riesgos aplicables están integradas e incorporadas en la organización interna para gestionar y supervisar los riesgos de TIC materiales identificados. A este respecto, las autoridades competentes evaluarán si la entidad demuestra:

    a. funciones y responsabilidades claras para la identificación, la evaluación, el seguimiento, la mitigación, la elaboración de información y la supervisión del riesgo de TIC material;

b. que las responsabilidades y funciones relacionadas con el riesgo de TIC se comunican, se asignan y se integran claramente en todas las partes (por ejemplo, líneas de negocio, TIC) y procesos pertinentes de la organización, incluidas las funciones y responsabilidades de recopilación y agregación de la información de riesgos y su comunicación a la alta dirección o al órgano de dirección;
c. que las actividades de gestión de riesgos de TIC se realizan con recursos humanos y técnicos suficientes y cualitativamente apropiados. A fin de evaluar la credibilidad de los planes de mitigación de riesgos aplicables, las autoridades competentes también evaluarán si la entidad ha asignado suficiente presupuesto u otros recursos necesarios para su implementación;
d. un seguimiento y una respuesta adecuados del órgano de dirección en relación con los resultados importantesrecibidos de las funciones de control independientes en relación con el riesgo o riesgos de TIC, teniendo en cuenta la posible delegación de algunos aspectos a un comité, en su caso; y
e. que las excepciones a las regulaciones y políticas aplicables en materia de TIC se registran y se someten a una revisión documentada y a un proceso de comunicación por parte de la función de control independiente, con especial atención a los riesgos relacionados.

3.3.3 Cobertura y resultados de auditoría interna

51. Las autoridades competentes considerarán si la función de auditoría interna audita con eficacia el marco de control de riesgos de TIC aplicable y, para ello, examinará si:

a. el marco de control de riesgos de TIC se audita con la calidad, el detalle y la frecuencia requeridos y en consonancia con el tamaño, las actividades y el perfil de riesgo de TIC de la entidad;
b. el plan de auditoría incluye auditorías de los riesgos de TIC críticos identificados por la entidad;
c. los resultados importantes de la auditoría de TIC, incluidas las medidas acordadas, se comunican al órgano de dirección; y
d. los resultados de la auditoría de TIC, incluidas las medidas acordadas, son objeto de seguimiento y la alta dirección o el comité de auditoría revisan periódicamente los informes de progreso.

3.3.4 Controles de riesgos de TIC específicos para los riesgos de TIC materiales identificados

52. Las autoridades competentes evaluarán si la entidad cuenta con controles específicos para hacer frente a los riesgos de TIC materiales identificados. En las siguientes secciones se proporciona una lista no exhaustiva de los controles específicos que deberán tenerse en cuenta al evaluar los riesgos materiales identificados en el punto 3.2.3, que se asignaron a las siguientes categorías de riesgo de TIC:

a. Riesgos de disponibilidad y continuidad de las TIC;
b. Riesgos de seguridad de las TIC;
c. Riesgos de cambio de las TIC;
d. Riesgos de integridad de datos TIC;
e. Riesgos de externalización de las TIC.

(a) Controles para la gestión de los riesgos materiales de disponibilidad y continuidad de las TIC

53. Además de los requisitos de las Directrices de la ABE sobre el PRES (apartados 279-281), las autoridades competentes evaluarán si la entidad cuenta con un marco adecuado para identificar, entender, medir y mitigar los riesgos de disponibilidad y continuidad de las TIC.

54. Al llevar a cabo esta evaluación, las autoridades competentes considerarán, en particular, si el marco:

a. identifica los procesos críticos de las TIC y los sistemas de soporte de TIC pertinentes que deberían formar parte de los planes de resiliencia y continuidad del negocio con:

   i. un análisis exhaustivo de las dependencias entre los procesos de negocio críticos y los sistemas de soporte;

   ii. la determinación de los objetivos de recuperación de los sistemas de soporte de TIC (normalmente son determinados por el negocio o la regulación en términos de RTO y de RPO);

   iii. una planificación de contingencia apropiada que permita la disponibilidad, la continuidad y la recuperación de sistemas y servicios de TIC críticos con el fin de minimizar las interrupciones en las operaciones de una entidad dentro de unos límites aceptables.

b. tiene políticas y estándares en materia de resiliencia de negocio y del entorno de control de la continuidad, así como controles operacionales que incluyen:

   i. medidas para evitar que un único escenario, incidente o desastre pueda afectar tanto a los sistemas de producción como a los de recuperación de TIC;

   ii. procedimientos de copia de seguridad y recuperación de los sistemas de TIC para *software* y datos críticos, que garanticen que estas copias de seguridad se almacenan en una ubicación segura y lo suficientemente alejada, de modo que un incidente o un desastre no puedan destruir o corromper estos datos críticos;

   iii. soluciones de monitorización para la detección oportuna de incidentes de disponibilidad o continuidad de las TIC;

   iv. un proceso documentado de gestión y escalamiento de incidentes, que también proporcione orientación sobre las diferentes funciones y responsabilidades en materia de gestión y escalamiento de incidentes, los miembros del comité o comités de crisis y la cadena de mando en caso de emergencia;

   v. medidas físicas para proteger la infraestructura crítica de TIC de la entidad (por ejemplo, centros de datos) de los riesgos ambientales (por ejemplo, inundaciones y otros desastres naturales) así como para garantizar un entorno operativo adecuado para los sistemas de TIC (por ejemplo, aire acondicionado);

   vi. procesos, funciones y responsabilidades para asegurar que también los sistemas y servicios de TIC externalizados estén cubiertos por soluciones y planes adecuados de continuidad y resiliencia del negocio;

vii. planificación de la capacidad y rendimiento en materia de TIC y soluciones de monitorización de los sistemas y servicios de TIC críticos con requisitos de disponibilidad definidos, a fin de detectar de manera oportuna limitaciones de rendimiento y capacidad importantes;

viii. soluciones para proteger las actividades o servicios críticos en internet (por ejemplo, servicios de banca electrónica), cuando sea necesario y apropiado, contra la denegación del servicio y otros ciberataques desde internet, dirigidos a impedir o interrumpir el acceso a estas actividades y servicios.

c. prueba las soluciones de disponibilidad y continuidad de las TIC frente a una serie de escenarios realistas que incluyen ciberataques, pruebas de conmutación y pruebas de copias de seguridad de *software* y datos críticos que:

i. se planifican, formalizan y documentan y sus resultados se utilizan para reforzar la eficacia de las soluciones de disponibilidad y continuidad de las TIC;

ii. implican a las partes interesadas y las funciones dentro de la organización, como la gestión de líneas de negocio, incluidos los equipos de continuidad del negocio, de incidentes y de respuesta a crisis, así como a terceros que sean relevantes para el ecosistema;

iii. implican de manera adecuada a la alta dirección y al órgano de dirección (por ejemplo, como parte de los equipos de gestión de crisis), que son informados de los resultados de las pruebas.

(b) Controles para la gestión de los riesgos de seguridad de las TIC materiales

55. Las autoridades competentes evaluarán si la entidad cuenta con un marco eficaz para identificar, entender, medir y mitigar el riesgo de seguridad de las TIC. En particular, al llevar a cabo esta evaluación, las autoridades competentes tendrán en cuenta si el marco contempla:

a. funciones y responsabilidades claramente definidas sobre:

i. la persona, personas o comités responsables de la gestión ordinaria de la seguridad de las TIC y la elaboración de las políticas generales en la materia, prestando atención a su necesaria independencia;
ii. el diseño, la ejecución, la gestión y el seguimiento de los controles de seguridad de las TIC;
iii. la protección de los sistemas y servicios de TIC críticos mediante la adopción de, por ejemplo, un proceso de evaluación de vulnerabilidades, la gestión de parches de *software*, la protección de los puntos finales (por ejemplo, *malware*), las herramientas de detección y prevención de intrusiones;
iv. el seguimiento, la clasificación y el tratamiento de incidentes de seguridad de las TIC externos o internos, incluida la respuesta a incidentes y la reanudación y la recuperación de los sistemas y servicios de TIC;
v. evaluaciones de amenazas regulares y proactivas para mantener los controles de seguridad apropiados;

b. una política de seguridad de las TIC que tenga en cuenta y, en su caso, cumpla las normas y principios de seguridad de las TIC reconocidos internacionalmente (por ejemplo, para la gestión de los derechos de acceso, el principio del menor privilegio, es decir, limitar el acceso al nivel mínimo que permita el funcionamiento normal; para diseñar una arquitectura de seguridad, el principio de «defensa en profundidad», es decir, mecanismos de seguridad en capas que aumentan la seguridad del sistema en su conjunto);

c. un proceso para identificar sistemas y servicios de TIC y requisitos de seguridad proporcionados, que contemplen el posible riesgo de fraude o posibles usos fraudulentos o abusos de datos confidenciales, junto con las expectativas de seguridad documentadas que deben respetarse para estos sistemas, servicios y datos identificados. Estos requisitos y expectativas tienen que estar en consonancia con la tolerancia al riesgo de la entidad y ser supervisados para asegurar su correcta aplicación;

d. un proceso documentado de gestión y escalamiento de incidentes, que describa las diferentes funciones y responsabilidades en la gestión y escalamiento de incidentes, los miembros del comité o comités de crisis y la cadena de mando en caso de emergencias de seguridad;

e. el registro de actividades de usuarios y de actividades administrativas que permita la monitorización eficaz y la detección y respuesta oportunas ante actividades no autorizadas, así como llevar a cabo o ayudar en investigaciones forenses de incidentes de seguridad. La entidad contará con políticas de registro de actividades que definan los tipos de registros apropiados que deben mantenerse y su periodo de conservación;

f. campañas o iniciativas de concienciación e información para informar a todos los niveles de la entidad sobre el uso seguro y la protección de los sistemas de TIC de la entidad y los principales riesgos de seguridad de las TIC (y otros riesgos) que deben conocer, en particular, sobre las amenazas cibernéticas existentes y cambiantes (por ejemplo, virus informáticos, posibles abusos o ataques internos o externos, ciberataques) y su papel en la mitigación de las violaciones de seguridad;

g. medidas de seguridad física adecuadas (por ejemplo, circuito cerrado de televisión, alarma antirrobo, puertas de seguridad) para impedir el acceso físico no autorizado a sistemas de TIC sensibles y críticos (por ejemplo, en centros de datos);

h. medidas para proteger los sistemas de TIC de los ataques de internet (es decir, ciberataques) u otras redes externas (por ejemplo, conexiones tradicionales de telecomunicaciones o conexiones con socios de confianza). Las autoridades competentes examinarán si el marco de la entidad considera:

    i. un proceso y soluciones para mantener una visión y un inventario completos y actualizados de todos los puntos externos de conexión a la red (por ejemplo, sitios web, aplicaciones de internet, WIFI, acceso remoto) a través de los cuales terceras partes podrían acceder sin autorización a los sistemas internos de TIC.

    ii. medidas de seguridad minuciosamente gestionadas y supervisadas (por ejemplo, cortafuegos, servidores *proxy*, intercambiadores de correo, antivirus y escáneres de contenido) para proteger el tráfico de red entrante y saliente (por ejemplo, correo

electrónico) y las conexiones externas a la red a través de las cuales terceras partes podrían acceder sin autorización a los sistemas internos de TIC;

iii. procesos y soluciones para proteger sitios web y aplicaciones que pueden ser atacados directamente desde internet o desde el exterior, que pueden servir como punto de entrada a los sistemas internos de TIC. En general, estos incluyen una combinación de prácticas de desarrollo seguras reconocidas, securización del sistema de TIC y prácticas de exploración de vulnerabilidades de dicho sistema, o la implementación de soluciones de seguridad adicionales como, por ejemplo, cortafuegos de aplicaciones o sistemas de detección de intrusiones (IDS) o de prevención de intrusiones (IPS);

iv. pruebas de penetración periódicas para evaluar la eficacia de las medidas y procesos de ciberseguridad y de seguridad tecnológica interna implementados. Estas pruebas las realizarán personal propio o expertos externos con la experiencia necesaria, los resultados de las pruebas se documentarán y las conclusiones se comunicarán a la alta dirección o al órgano de dirección. Cuando sea necesario y aplicable, la entidad utilizará estas pruebas para conocer dónde puede mejorar aún más los controles y procesos de seguridad o para obtener mayor certeza de su efectividad.

(c) Controles para la gestión de los riesgos materiales de cambio de las TIC

56. Las autoridades competentes evaluarán si la entidad cuenta con un marco eficaz para identificar, entender, medir y mitigar el riesgo de cambio de las TIC de acuerdo con la naturaleza, la escala y la complejidad de las actividades de la entidad y su perfil de riesgo de TIC. El marco de la entidad cubrirá los riesgos asociados con el desarrollo, la prueba y la aprobación de los cambios en los sistemas de TIC, incluyendo el desarrollo o el cambio de *software*, antes de migrar al entorno de producción y asegurará una gestión adecuada del ciclo de vida de las TIC. Al llevar a cabo esta evaluación, las autoridades competentes tendrán en cuenta, en particular, si el marco contempla:

a. procesos documentados para gestionar y controlar los cambios en los sistemas de TIC (por ejemplo, configuración y gestión de parches) y en los datos (por ejemplo, corrección de errores o correcciones de datos), que garanticen una implicación adecuada de la función de gestión del riesgo de TIC en aquellos cambios importantes en las TIC que puedan afectar significativamente al perfil de riesgo de TIC o a la exposición al riesgo de la entidad;

b. especificaciones sobre la necesaria separación de funciones durante las diferentes fases de los procesos de cambio de las TIC llevados a cabo (por ejemplo, diseño y desarrollo de soluciones, pruebas y aprobación de nuevos programas o cambios, migración e implementación en el entorno de producción y corrección de errores), con especial atención a la segregación de tareas y las soluciones implementadas para gestionar y controlar los cambios en los sistemas y datos de producción en materia de TIC por parte del personal de TIC (por ejemplo, desarrolladores, administradores de sistemas de TIC, administradores de bases de datos) o cualquier otra parte implicada (por ejemplo, usuarios de negocio, proveedores de servicios);

c. entornos de prueba que reflejen adecuadamente los entornos de producción;

d. un inventario de activos de las aplicaciones y los sistemas de TIC existentes en el entorno de producción, así como en el entorno de prueba y desarrollo, para que los cambios requeridos (por

ejemplo, actualizaciones de versiones, parches de sistemas y cambios de configuración) puedan ser gestionados, aplicados y monitorizados de manera adecuada para los sistemas de TIC implicados;

e. un proceso de seguimiento y gestión del ciclo de vida de los sistemas de TIC utilizados, para garantizar que continúan cumpliendo y dando soporte a las exigencias reales de gestión de riesgos y del negocio y para asegurar que las soluciones y sistemas de TIC utilizados siguen recibiendo soporte de sus proveedores, y que todo ello viene acompañado de procedimientos adecuados de ciclo de vida de desarrollo de *software* (SDLC).

f. un sistema de control de código fuente de *software* y procedimientos apropiados para prevenir cambios no autorizados en el código fuente del *software* que se desarrolle a nivel interno;

g. un proceso para llevar a cabo un análisis de seguridad y vulnerabilidad de sistemas y *software* de TIC modificados y nuevos, antes de ponerlos en producción y exponerlos a posibles ciberataques;

h. un proceso y soluciones para prevenir la divulgación no autorizada o no deseada de datos confidenciales, al reemplazar, archivar, descartar o destruir sistemas de TIC;

i. un proceso independiente de revisión y validación para reducir los riesgos de errores humanos al realizar cambios en los sistemas de TIC que puedan tener un efecto negativo importante en la disponibilidad, continuidad o seguridad de la entidad (por ejemplo, cambios importantes en la configuración de los cortafuegos).

(d) Controles para la gestión de los riesgos materiales de integridad de datos TIC

57. Las autoridades competentes evaluarán si la entidad cuenta con un marco eficaz para identificar, entender, medir y mitigar el riesgo para la integridad de datos TIC de acuerdo con la naturaleza, la escala y la complejidad de las actividades de la entidad y su perfil de riesgo de TIC. El marco de la entidad considerará los riesgos asociados con la preservación de la integridad de los datos almacenados y procesados por los sistemas de TIC. Al llevar a cabo esta evaluación, las autoridades competentes tendrán en cuenta, en particular, si el marco contempla:

a. una política que defina las funciones y responsabilidades para gestionar la integridad de los datos en los sistemas de TIC (por ejemplo, arquitecto de datos, responsables de datos[6], custodios de datos[7], propietarios/administradores de datos[8]) y proporcione orientación sobre qué datos son críticos desde la perspectiva de la integridad de los datos y deberán estar sujetos a controles específicos de TIC (por ejemplo, controles de validación de entrada automatizados, controles de transferencia de datos, conciliaciones, etc.) o revisiones (por ejemplo, una verificación de compatibilidad con la arquitectura de datos) en las diferentes fases del ciclo de vida de los datos de las TIC;

b. una arquitectura de datos, un modelo de datos o un diccionario de datos documentados, que se validen con los actores relevantes del negocio y de las TIC para contribuir a la necesaria coherencia

[6] El responsable de datos se encarga del tratamiento y el uso de los datos.

[7] El custodio de datos se encarga de la custodia, el transporte y el almacenamiento seguros de los datos.

[8] El administrador de datos es responsable de la gestión y la adecuación de los elementos de datos, tanto del contenido como de los metadatos.

de datos en los sistemas de TIC y para asegurar que la arquitectura de datos, el modelo de datos o el diccionario de datos permanecen alineados con las necesidades del negocio y de la gestión de riesgos;

c. una política en relación con el uso permitido y la dependencia de las soluciones informáticas de usuario final, en particular, con respecto a la identificación, el registro y la documentación de soluciones informáticas de usuario final importantes (por ejemplo, por procesar datos importantes) y los niveles de seguridad esperados para prevenir modificaciones no autorizadas, tanto en la propia herramienta como en los datos almacenados en ella;

d. procesos de gestión de excepciones documentados para resolver los problemas de integridad de los datos TIC identificados de acuerdo con su criticidad y sensibilidad.

58. Por lo que respecta a las entidades supervisadas incluidas dentro del ámbito de aplicación de los principios del CSBB 239 para una eficaz agregación de datos sobre riesgos y presentación de informes de riesgos[9], las autoridades competentes revisarán el análisis de riesgos de la entidad relativo a sus capacidades de agregación de datos y de comunicación de riesgos comparándolas con los principios y la documentación preparada al respecto, teniendo en cuenta el calendario de aplicación y las disposiciones transitorias que se recogen en estos principios.

(e) Controles para la gestión de los riesgos materiales de externalización de las TIC

59. Las autoridades competentes evaluarán si la estrategia de externalización de la entidad, de conformidad con los requisitos de las Directrices del CSBE sobre externalización (2006) y con el requisito del apartado 85, letra d), de las Directrices de la ABE sobre el PRES, se aplica adecuadamente a la externalización de las TIC, incluida la externalización intragrupo que presta servicios de TIC dentro del grupo. Al evaluar los riesgos de externalización de las TIC, las autoridades competentes tendrán en cuenta que estos riesgos también se pueden tratar como parte de la evaluación de los riesgos operacionales inherentes con arreglo al apartado 240, letra j), de las Directrices de la ABE sobre el PRES, a fin de evitar la duplicación de trabajo o el doble cómputo.

60. En particular, las autoridades competentes evaluarán si la entidad cuenta con un marco eficaz para identificar, entender y medir el riesgo de externalización de las TIC y, en particular, si dispone de controles y un entorno de control para mitigar los riesgos relacionados con los servicios de TIC externalizados que sean proporcionales al tamaño, las actividades y el perfil de riesgo de TIC de la entidad y que incluyan:

a. una evaluación del impacto de la externalización de las TIC sobre la gestión de riesgos de la entidad en relación con el uso de proveedores de servicios (por ejemplo, proveedores de servicios en la nube) y sus servicios durante el proceso de adquisición, que se documenta y es tenido en cuenta por la alta dirección o el órgano de dirección a la hora de tomar una decisión sobre si externalizar los servicios o no. La entidad revisará las políticas de gestión de riesgos de TIC y el entorno de control y los controles de TIC del proveedor de servicios para asegurarse de que cumplen con los

[9] Comité de Supervisión Bancaria de Basilea, Principios para una eficaz agregación de datos sobre riesgos y presentación de informes de riesgos, enero de 2013, disponible en línea: http://www.bis.org/publ/bcbs239_es.pdf.

objetivos internos de gestión de riesgos de la entidad y su apetito de riesgo. Esta revisión se actualizará periódicamente durante el periodo contractual de la externalización, teniendo en cuenta las características de los servicios subcontratados;

b. un seguimiento de los riesgos de TIC de los servicios externalizados durante el periodo contractual de la externalización como parte de la gestión de riesgos de la entidad, que sirva de base para la presentación de informes de gestión de riesgos de TIC de la entidad (por ejemplo, informes de continuidad del negocio, informes de seguridad).

c. un seguimiento y comparación de los niveles de servicio recibidos con los niveles de servicio contractualmente acordados que deben formar parte del contrato de externalización o del acuerdo de nivel de servicio (SLA); y

d. personal, recursos y competencias adecuados para vigilar y gestionar los riesgos de TIC de los servicios externalizados.

3.4 Resumen de resultados y puntuación

61. Una vez realizada la evaluación anterior, las autoridades competentes se formarán una opinión sobre el riesgo de TIC de la entidad. Esta opinión se reflejará en un resumen de resultados que las autoridades competentes tendrán en cuenta al asignar la puntuación de riesgo operacional que figura en el cuadro 6 de las Directrices de la ABE sobre el PRES. Las autoridades competentes basarán su opinión sobre los riesgos de TIC materiales en las siguientes consideraciones, que deben servir para la evaluación del riesgo operacional:

a. Consideraciones sobre el riesgo

   i. El perfil de riesgo de TIC de la entidad y sus exposiciones a dicho riesgo;
   ii. Los sistemas y servicios críticos de TIC identificados; y
   iii. La materialidad del riesgo de TIC en relación con los sistemas de TIC críticos.

b. Consideraciones sobre la gestión y los controles

   i. Si existe coherencia entre la política y la estrategia de gestión del riesgo de TIC de la entidad y su estrategia general y apetito de riesgo;
   ii. Si el marco organizativo de la gestión del riesgo de TIC es sólido, con responsabilidades claras y una separación clara de tareas entre el personal que asume el riesgo y las funciones de gestión y control;
   iii. Si los sistemas de medición, seguimiento e información de riesgos de TIC son adecuados; y
   iv. Si los marcos de control de los riesgos de TIC materiales son sólidos.

62. Si las autoridades competentes consideran que el riesgo de TIC es material y deciden evaluar y puntuar este riesgo como una subcategoría del riesgo operacional, la tabla siguiente (tabla 1) proporciona las consideraciones para la puntuación del riesgo de TIC.

Tabla 1: Consideraciones supervisoras para asignar una puntuación de riesgo de TIC

Puntuación del riesgo	Opinión supervisora	Consideraciones para el riesgo inherente	Consideraciones para la gestión y controles adecuados
1	No existe un riesgo apreciable de impacto prudencial significativo en la entidad teniendo en cuenta el nivel de riesgo inherente y la gestión y controles.	• Las fuentes de información que se han de considerar conforme al apartado 37 no revelaron ninguna exposición significativa al riesgo de TIC. • La naturaleza del perfil de riesgo de TIC de la entidad, junto con la revisión de los sistemas de TIC críticos y los riesgos de TIC materiales para los sistemas y servicios de TIC, no han revelado ningún riesgo de TIC material.	• La política y la estrategia de riesgo de TIC de la entidad son proporcionales a su estrategia general y a su apetito de riesgo. • El marco organizativo para el riesgo de TIC es sólido, con responsabilidades claras y una separación clara de tareas entre el personal que asume el riesgo y las funciones de gestión y control. • Los sistemas de medición, seguimiento e información de riesgos de TIC son adecuados. • El marco de control del riesgo de TIC es sólido.
2	Existe un bajo riesgo de impacto prudencial significativo en la entidad teniendo en cuenta el nivel de riesgo inherente y la gestión y controles.	• Las fuentes de información que se han de considerar conforme al apartado 37 no revelaron ninguna exposición significativa al riesgo de TIC. • La naturaleza del perfil de riesgo de TIC de la entidad, junto con la revisión de los sistemas de TIC críticos y los riesgos de TIC materiales para los sistemas y servicios de TIC, han revelado una exposición limitada al riesgo de TIC (por ejemplo, no más de 2 de las 5 categorías de riesgo de TIC predefinidas).	
3	Existe un riesgo medio de impacto prudencial significativo en la entidad teniendo en cuenta el nivel de riesgo inherente y la gestión y controles.	• Las fuentes de información que se han de considerar conforme al apartado 37 revelaron indicios de posibles exposiciones significativas al riesgo de TIC. • La naturaleza del perfil de riesgo de TIC de la entidad, junto con la revisión de los sistemas de TIC críticos y los riesgos de TIC materiales para los sistemas y servicios de TIC, han revelado una exposición elevada al riesgo de TIC (por ejemplo, 3 o más de las 5 categorías de riesgo de TIC predefinidas).	

4	Existe un alto riesgo de impacto prudencial significativo en la entidad teniendo en cuenta el nivel de riesgo inherente y la gestión y controles.	• Las fuentes de información que se han de considerar conforme al apartado 37 revelaron múltiples indicios de exposiciones significativas al riesgo de TIC. • La naturaleza del perfil de riesgo de TIC de la entidad, junto con la revisión de los sistemas de TIC críticos y los riesgos de TIC materiales para los sistemas y servicios de TIC, han revelado una exposición muy elevada al riesgo de TIC (por ejemplo, 4 o 5 de las 5 categorías de riesgo de TIC predefinidas).	

Anexo - Taxonomía de riesgos de TIC

Cinco categorías de riesgo de TIC con una lista no exhaustiva de riesgos de TIC que podrían generar pérdidas muy graves o tener un alto impacto operacional, reputacional o financiero

Categorías de riesgo de TIC	Riesgos de TIC (detalle no exhaustivo[10])	Descripción del riesgo	Ejemplos
Riesgos de disponibilidad y continuidad de las TIC	Gestión inadecuada de la capacidad	La falta de recursos (por ejemplo, *hardware*, *software*, personal, proveedores de servicios) puede traducirse en una incapacidad para ajustar el servicio a fin de hacer frente a las necesidades del negocio, en interrupciones del sistema, en el deterioro del servicio o en errores operacionales.	• Un déficit de capacidad puede afectar a las ratios de transmisión y a la disponibilidad de la red (internet) para servicios como la banca por internet. • La falta de personal (interno o externo) puede resultar en interrupciones del sistema o errores operacionales.
	Fallos del sistema de TIC	Una pérdida de disponibilidad debido a fallos de *hardware*.	• Fallo/mal funcionamiento del almacenamiento (discos duros), servidor u otros equipos de TIC causado, por ejemplo, por falta de mantenimiento.
		Una pérdida de disponibilidad debida a fallos y errores de *software*.	• Bucle infinito en el *software* de aplicaciones que impide la ejecución de las operaciones. • Interrupciones debidas al uso continuado de sistemas y soluciones de TIC obsoletos, que ya no cumplen con los requisitos actuales de disponibilidad y resiliencia o ya no son mantenidos por sus proveedores.
	Planificación inadecuada de la continuidad de TIC y de recuperación frente a desastres	Fallo de las soluciones planificadas de disponibilidad o continuidad de TIC o de recuperación frente a desastres (por ejemplo, centro de datos de recuperación ante caídas) cuando se activan en respuesta a un incidente.	• Las diferencias de configuración entre el centro de datos primario y secundario pueden resultar en la incapacidad del centro de datos de recuperación ante caídas para mantener la continuidad planificada del servicio.

[10] Los riesgos de TIC se enumeran en la categoría de riesgo a la que más afectan, pero pueden afectar a otras categorías de riesgo

Categorías de riesgo de TIC	Riesgos de TIC (detalle no exhaustivo[10])	Descripción del riesgo	Ejemplos
	Ciberataques disruptivos y destructivos	Ataques con diferentes propósitos (por ejemplo, activismo, chantaje), que se traducen en una sobrecarga de los sistemas y de la red, impidiendo que los usuarios legítimos puedan acceder a los servicios informáticos en línea.	• Los ataques distribuidos de denegación de servicio (DDoS) se realizan mediante una multitud de sistemas informáticos en internet controlados por un pirata informático que envía una gran cantidad de solicitudes de servicio aparentemente legítimas a los servicios de internet (por ejemplo, banca electrónica).
Riesgos de seguridad de las TIC	Ciberataques y otros ataques externos basados en TIC	Ataques realizados desde internet o redes externas con diferentes propósitos (por ejemplo, fraude, espionaje, activismo/sabotaje, ciberterrorismo) aplicando distintas técnicas (por ejemplo, ingeniería social, intentos de intrusión a través de la explotación de vulnerabilidades, distribución de *software* malicioso) que se traducen en la toma de control de los sistemas de TIC internos.	Diferentes tipos de ataques: • Amenaza persistente avanzada (APT) para tomar el control de sistemas internos o robar información (por ejemplo, información relacionada con robo de identidad, información de tarjetas de crédito). • *Software* malicioso (por ejemplo, *ransomware*) que cifra datos con fines de chantaje. • Infección de los sistemas internos de TIC con troyanos para cometer actos maliciosos de manera oculta. • Explotación de vulnerabilidades de los sistemas de TIC o de aplicaciones (web) (por ejemplo, inyección SQL ...) para acceder a los sistemas internos de TIC.
		Ejecución de operaciones de pago fraudulentas por parte de piratas informáticos mediante la violación o la elusión de la seguridad de los servicios de banca electrónica y de pago o mediante el ataque y la explotación de vulnerabilidades de seguridad en los sistemas de pago internos de la entidad.	• Ataques contra servicios de banca electrónica o de pago con el objetivo de realizar operaciones no autorizadas. • Creación y envío de operaciones de pago fraudulentas desde los sistemas de pago internos de la entidad (por ejemplo, mensajes SWIFT fraudulentos).
		Ejecución de operaciones de valores fraudulentas por parte de piratas informáticos mediante la violación o la elusión de la seguridad de los servicios de banca electrónica que también proporcionan acceso a las	• Ataques de bombardeo y descarga en los que los atacantes obtienen acceso a cuentas de valores de banca electrónica de clientes y envían órdenes de compra o venta fraudulentas para influir en el

Categorías de riesgo de TIC	Riesgos de TIC (detalle no exhaustivo[10])	Descripción del riesgo	Ejemplos
		cuentas de valores del cliente.	precio de mercado o realizar ganancias basadas en posiciones de valores previamente establecidas.
		Ataques a las conexiones de comunicación y conversaciones de todo tipo en sistemas de TIC con el objetivo de recopilar información o cometer fraude.	• Escuchas secretas (*eavesdropping)*/interceptación de transmisiones sin protección de datos de autenticación en texto sin formato.
	Seguridad interna de las TIC inadecuada	Obtención de acceso no autorizado a los sistemas de TIC críticos desde dentro de la entidad con diferentes propósitos (por ejemplo, fraude, realización y ocultación de actividades comerciales fraudulentas, robo de datos, activismo/sabotaje) mediante diversas técnicas (por ejemplo, abuso o aumento de privilegios, robe de identidad, ingeniería social, explotación de vulnerabilidades en sistemas de TIC, distribución de *software* malicioso).	• Instalar registradores de teclas (*keyloggers*) para robar identificadores de usuario y contraseñas con el fin de obtener acceso no autorizado a datos confidenciales o cometer fraude. • Descifrado o adivinación de contraseñas débiles para obtener derechos de acceso ilegítimos o elevados. • El administrador del sistema utiliza sistemas operativos o utilidades de base de datos (para modificaciones directas en la base de datos) para cometer fraude.
		Manipulaciones no autorizadas de las TIC debido a procedimientos y prácticas inadecuados de gestión de accesos a las TIC.	• No se inhabilitan o borran cuentas innecesarias, como las del personal que cambió de funciones o que ha dejado la entidad, incluidos invitados o proveedores que ya no necesitan acceso, lo que proporciona acceso no autorizado a los sistemas de TIC. • Concesión de derechos y privilegios de acceso excesivos, permitiendo accesos no autorizados o que se oculten actividades deshonestas.
		Amenazas a la seguridad debido a la falta de conciencia de seguridad que hace que los empleados no entiendann, descuiden o no cumplan las políticas y procedimientos de seguridad de TIC.	• Empleados que son engañados para ayudar a cometer un ataque (es decir, ingeniería social). • Malas prácticas con respecto a las credenciales: compartir contraseñas, usar contraseñas «fáciles» de adivinar, usar la misma contraseña para muchos propósitos diferentes, etc.

Categorías de riesgo de TIC	Riesgos de TIC (detalle no exhaustivo[10])	Descripción del riesgo	Ejemplos
			• Almacenamiento de datos confidenciales no cifrados en portátiles y soluciones de almacenamiento de datos portátiles (por ejemplo, dispositivos USB) que se pueden perder o robar.
		Almacenamiento o transferencia no autorizados de información confidencial fuera de la entidad.	• Personas que roban o filtran deliberadamente o envían clandestinamente información confidencial a personas no autorizadas o al público en general.
	Seguridad física de las TIC inadecuada	Mal uso o robo de los activos de TIC a través del acceso físico que causa daños o pérdida de activos o de datos o que hace posibles otras amenazas.	• Intrusión física en edificios de oficinas o centros de datos para robar equipos informáticos (por ejemplo, ordenadores de sobremesa, ordenadores portátiles, soluciones de almacenamiento) o copiar datos mediante el acceso físico a los sistemas de TIC.
		Daños deliberados o accidentales a activos físicos de TIC causados por terrorismo, accidentes o manipulaciones desafortunadas/erróneas por parte del personal de la entidad o de terceros (proveedores, reparadores).	• Terrorismo físico (es decir, bombas terroristas) o sabotaje de activos de TIC. • Destrucción del centro de datos causada por incendio, fugas de agua u otros factores.
		Protección física insuficiente frente a desastres naturales que ocasionan la destrucción parcial o total de los sistemas/centros de datos de TIC.	• Terremotos, calor extremo, tormentas de viento, fuertes tormentas de nieve, inundaciones, incendios, relámpagos.
Riesgos de cambio de las TIC	Control inadecuado de los cambios en los sistemas de TIC y del desarrollo de las TIC	Incidentes causados por errores no detectados o vulnerabilidades al cambiar, entre otros, *software*, sistemas y datos de TIC (por ejemplo, efectos imprevistos de un cambio o un cambio mal gestionado debido a la falta de pruebas o prácticas inapropiadas de gestión del cambio).	• Puesta en producción de *software* insuficientemente probado o cambios de configuración con efectos adversos imprevistos en los datos (por ejemplo, corrupción, eliminación) o en el rendimiento de los sistemas de TIC (por ejemplo, colapso, deterioro del rendimiento). • Cambios incontrolados en los sistemas o datos de TIC en el entorno de producción. • Puesta en producción de sistemas de TIC y aplicaciones de internet mal protegidos, creando

Categorías de riesgo de TIC	Riesgos de TIC (detalle no exhaustivo[10])	Descripción del riesgo	Ejemplos
			oportunidades para que los piratas informáticos ataquen los servicios de internet prestados o accedan sin autorización a los sistemas de TIC internos. • Cambios incontrolados en el código fuente de *software* desarrollado internamente. • Pruebas insuficientes debido a la falta de entornos de prueba adecuados.
	Arquitectura de TIC inadecuada	Una gestión deficiente de la arquitectura de TIC al diseñar, construir y mantener sistemas de TIC (por ejemplo, *software*, *hardware*, datos) puede dar lugar, con el tiempo, a sistemas de TIC complejos, difíciles, costosos de manejar y rígidos que ya no están suficientemente alineados con las necesidades de negocio y se quedan obsoletos para satisfacer los requisitos reales de gestión de riesgos.	• Cambios inadecuadamente gestionados en los sistemas, *software* o datos de TIC durante un periodo de tiempo prolongado, que da lugar a sistemas y arquitecturas de TIC complejos, heterogéneos y difíciles de gestionar, que tienen numerosos efectos negativos para la gestión del negocio y del riesgo (por ejemplo, falta de flexibilidad y agilidad, incidentes y fallos de TIC, altos costes operativos, debilitamiento de la seguridad y resiliencia de TIC, reducción de la calidad de los datos y menor capacidad de información). • Excesiva personalización y ampliación de paquetes de *software* comercial con *software* desarrollado internamente, lo que se traduce en incapacidad para implementar futuras versiones y actualizaciones del *software* comercial y el riesgo de que ya no cuente con el soporte del proveedor.
	Gestión inadecuada del ciclo de vida y de los parches	Falta de mantenimiento de un inventario adecuado de todos los activos de TIC que favorezca y se complemente con unas prácticas sólidas de gestión del ciclo de vida y de parches. Esto da lugar a sistemas de TIC insuficientemente parcheados (y, por lo tanto, más	• Sistemas de TIC no parcheados y obsoletos que pueden repercutir de manera negativa sobre la gestión del negocio y del riesgo (por ejemplo, falta de flexibilidad y agilidad, interrupciones de las TIC, menor seguridad y resiliencia de las TIC).

Categorías de riesgo de TIC	Riesgos de TIC (detalle no exhaustivo[10])	Descripción del riesgo	Ejemplos
		vulnerables) y obsoletos que pueden no responder a las necesidades del negocio y de gestión de riesgos.	
Riesgos de integridad de datos TIC	Tratamiento o manipulación disfuncional de datos TIC	Debido a errores o fallos de sistema, comunicación o aplicación, o a un proceso mal ejecutado de extracción, transferencia y carga (ETC) de datos, los datos podrían corromperse o perderse.	• Error en el sistema de TI en el procesamiento por lotes (*batch*), que origina saldos incorrectos en las cuentas bancarias del cliente • Consultas erróneamente ejecutadas • Pérdida de datos debido a un error de replicación (copia de seguridad).
	Controles de validación de datos mal diseñados en sistemas de TIC.	Errores relacionados con la ausencia o ineficacia de controles automatizados de entrada y aceptación de datos (por ejemplo, para datos de terceros utilizados), transferencia de datos, procesamiento y controles de datos de salida en los sistemas de TIC (por ejemplo, controles de validez de datos, conciliaciones de datos)	• Formato o validación insuficientes o inválidos de entradas de datos en aplicaciones o interfaces de usuario. • Ausencia de controles de conciliación de los datos de salida producidos. • Ausencia de controles en los procesos de extracción de datos ejecutados (por ejemplo, consultas de base de datos) que dan lugar a datos erróneos • Uso de datos externos defectuosos.
	Cambios de datos mal controlados en los sistemas de TIC de producción	Errores introducidos en los datos por la falta de controles que aseguren que las manipulaciones de datos realizadas en los sistemas de TIC de producción son correctas y están justificadas	• Desarrolladores o administradores de bases de datos que acceden directamente y cambian los datos en los sistemas de TIC de producción de una manera no controlada, por ejemplo, en el caso de un incidente de TIC
	Arquitectura de datos, flujos de datos, modelos de datos o diccionarios de datos mal gestionados o diseñados	Arquitecturas de datos, modelos de datos, flujos de datos o diccionarios de datos mal gestionados que pueden dar lugar a múltiples versiones de los mismos datos en los sistemas de TIC, que dejan de ser coherentes ya que los modelos de datos o las definiciones de datos se aplican de forma diferente o el proceso subyacente de generación o cambio de los datos es distinto.	• La existencia de diferentes bases de datos de clientes por producto o unidad de negocio con diferentes definiciones de datos y campos, lo que da lugar a problemas de conciliación y a dificultades de comparación a la hora de integrar los datos de clientes a nivel de toda la entidad financiera o grupo.
Riesgos de	Resiliencia	Falta de disponibilidad de servicios críticos de TIC,	• Falta de disponibilidad de servicios básicos como

Categorías de riesgo de TIC	Riesgos de TIC (detalle no exhaustivo[10])	Descripción del riesgo	Ejemplos
externalización de las TIC	insuficiente de servicios proporcionados por terceros o por otra entidad del grupo	servicios de telecomunicaciones y servicios de electricidad externalizados. Pérdida o corrupción de datos críticos/sensibles confiados al proveedor de servicios	consecuencia de fallos en los sistemas o aplicaciones de TIC de los proveedores (externalizados). • Interrupción de los enlaces de telecomunicaciones. • Falta de suministro eléctrico.
	Gestión inadecuada de la externalización	Importantes deterioros o fallos del servicio debido a que la preparación o los procesos de control del proveedor de los servicios externalizados son ineficientes. Una gestión ineficaz de la externalización puede traducirse en una falta de habilidades y capacidades apropiadas para identificar, evaluar, mitigar y seguir íntegramente los riesgos de TIC y puede limitar las capacidades operacionales de las entidades.	• Los procedimientos de gestión de incidentes, los mecanismos de control contractuales y las garantías incorporadas en el acuerdo con el proveedor de servicios son deficientes e incrementan la dependencia de personas clave de terceros y proveedores. • Unos controles inadecuados de la gestión del cambio en relación con el entorno de TIC de los proveedores de servicios pueden causar deterioros o fallos importantes en el servicio.
	Seguridad insuficiente de terceros o de otra entidad del grupo	Pirateo de los sistemas de TIC de proveedores de servicios, con un impacto directo en los servicios externalizados o en los datos críticos/confidenciales almacenados en el proveedor de servicios. El personal del proveedor de servicios obtiene acceso no autorizado a datos críticos/sensibles almacenados en el proveedor de servicios.	• Pirateo de proveedores de servicios por parte de delincuentes o terroristas, como punto de entrada a los sistemas de TIC de las entidades o para acceder/destruir datos críticos o sensibles almacenados en el proveedor de servicios. • Personal malicioso en el proveedor de servicios intenta robar y vender datos sensibles.